

REMARKS

Prior to this amendment, Claims 1-20 were pending in the application. By this amendment, Claims 1-20 are canceled and new claims 21-44 are added. Hence, Claims 21-44 are pending in the application.

SUMMARY OF THE REJECTIONS/OBJECTIONS

Claim 4 was previously rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 3-14 and 16-20 were rejected under 35 U.S.C. § 102(e) as being anticipated by Cheng et al. ("*Cheng*"; U.S. Pat. No. 6,823,462).

RESPONSE TO REJECTIONS NOT BASED ON THE PRIOR ART

Indefiniteness Rejections

Claim 4 was previously rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant has canceled Claim 4 and requests withdrawal of the rejection.

RESPONSE TO REJECTIONS BASED ON PRIOR ART

Rejections under 35 U.S.C. § 102(e)

(I) Claims 1, 3-14 and 16-20

Claims 1, 3-14 and 16-20 were rejected under 35 U.S.C. § 102(e) as anticipated by *Cheng*. Applicant has canceled Claims 1-20 and requests withdrawal of the rejection.

NEW CLAIMS 21-44

Applicant has added new claims 21-44, including new independent claims 21, 34 and 41-44. These new independent claims contain language and limitations similar to previous independent claims 1, 14 and 17-20, except Applicant has replaced the term “proxies” with the term “network addresses” to improve the clarity and readability of the new independent claims.

Applicant believes the new claims 21-44 are allowable over the art cited in the previous Office Action for the reasons stated below, and Applicant requests that a timely Notice of Allowance be issued in this case.

CLAIMS 21-44 ARE ALLOWABLE OVER *CHENG*

The Office Action alleges the “security policy” of *Cheng* anticipates the claim language of the instant application describing a “description of network traffic... wherein the [description] comprises a [set] of proxies.”

While Applicant does not agree with the above assertion, Applicant has replaced the term “proxies” with “network addresses” in the new independent claims to improve the clarity and readability of the new claims and clearly indicate the novelty of the approaches contained within.

Applicant thanks the Examiner for the telephone interview conducted on April 13, 2006 and will briefly restate the reasons new claims 21-44 are allowable over *Cheng* as discussed during the interview.

Cheng is directed to an approach for determining a security policy in a virtual private network where the endpoints of the tunnel are known. Clearly, *Cheng* is concerned with how traffic between known endpoints is to be protected, not about determining which endpoints should have security policies applied. This is clear from the following language in *Cheng*:

In step 330, a tunnel definition database in the server node 110A is configured so that the server node 110A has one tunnel definition for each of the plurality of tunnels 120 associated with a group name. As stated in the Background Information section, the tunnel definition establishes the end points of that particular tunnel 120.

Cheng, col. 5, lines 62-67.

Further, in *Cheng*:

The VPN security policy typically describes the characteristics of the protection for a particular traffic profile. That is, the VPN security policy describes the protection of the flow of data between the plurality of nodes 110 establishing the tunnel 120 of the virtual private network. Furthermore, the VPN security policy describes how the traffic is to be protected, e.g., authentication, encryption, transforms, key lengths and lifetimes, etc.

Cheng, col. 6, lines 53-60.

There is nothing in *Cheng* that teaches, anticipates or suggests an approach for determining which end hosts should have security applied to them. The clear novelty of one of the claimed approaches is that hosts unknown to one endpoint may be determined to be secure. One example is that the claimed approach allows a host to securely

communicate with a private address, such as private addresses behind a NAT or non-exposed hosts behind a firewall. This is

Further, *Cheng* does not anticipate, teach or suggest “creating and storing a third description of network traffic that is to be protected based on determining a logical intersection of the first description of network traffic and the second description of network traffic, wherein the step of creating and storing a third description further comprises the step of determining a largest common subset between the first set of network addresses and the second set of network addresses; and establishing the secure connection between the first network device and the second network device based on the third description of network traffic.”

This is shown by, among other things, *Cheng* specifically discussing the use of IKE Phase 2:

As stated above, IKE is used to establish security associations in order to activate a particular tunnel 120. IKE is made up of two phases defined within an Internet Security Association and Key Management Protocol (ISAKMP) framework. The ISAKMP framework establishes the security associations and cryptographic keys. The first phase establishes the security associations between the plurality of nodes 110 establishing a particular tunnel. IKE assumes that no secure channel, i.e., tunnel, currently exists and therefore it must initially establish one to protect any ISAKMP messages. The second phase refers to the negotiation of the security association for Internet Protocol (IP) security. Upon the successful completion of the negotiation of the phase two security association, data may be transferred between the plurality of nodes 110 establishing the tunnel 120.

Cheng, col. 7, lines 16-30.

This actually teaches away from the claimed approaches, because IKE tunnels have known endpoints. There is no suggestion in *Cheng* for a secure connection to be established based upon a largest common subset of network addresses, because the

network addresses of the endpoints are already known. The claimed approach is not negotiating how the data is to be transferred, as opposed to *Cheng*.

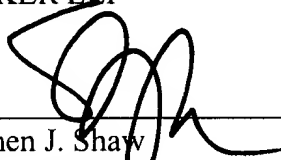
CONCLUSION

For at least the reasons indicated above, Applicants submit that pending Claims 21-44 present patentable subject matter, and are in condition for allowance. Therefore, Applicants respectfully request that a timely Notice of Allowance be issued in this case. If the Examiner has questions regarding this case, the Examiner is invited to contact Applicant's undersigned representative.

Please charge any shortages in fees due in connection with the filing of this paper, including extension of time fees, or credit any overages to Deposit Account No. 50-1302.

Respectfully Submitted,

HICKMAN PALERMO TRUONG &
BECKER LLP



Stephen J. Shaw
Reg. No. 56,442

Date: April 19, 2006

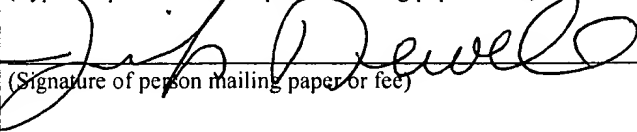
(408) 414-1080, Ext. 231
Fax: (408) 414-1076
2055 Gateway Place, Suite 550
San Jose, CA 95110-1089

Express Mail" mailing label number EV 835722181 US Date of Deposit: April 19, 2006

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Jennifer Newell

(Typed or printed name of person mailing paper or fee)



(Signature of person mailing paper or fee)